Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended): A method of detecting critical file changes, comprising:

reading an event ~~events~~ representing ~~various~~ at least one ~~types of~~ system call ~~calls~~;

routing the event to ~~an appropriate~~ a template, the event ~~having~~ comprising multiple parameters and the template comprising a sequence of connected logic nodes comprising at least one input node, at least one filter node, and at least one output node;

filtering the event, based on the sequence of logic nodes of the template, as ~~either~~ a possible intrusion based on the multiple parameters and either dropping the event or outputting the event, the filtering comprising:

determining a filename based on the event;

outputting the event for each event indicating modification of a critical file based upon the determined filename; and

creating an intrusion alert ~~if an~~ for each event [[is]] output from said filtering ~~step~~.

2. (Currently Amended): The method of claim 1, wherein said filtering ~~step~~ further comprises providing the event to the determining a filename ~~outputs an event~~ [[if]] for each event comprising [[the]] a ~~parameters indicate that the~~ a parameter indicating modification of a permission ~~bits~~ bit on a file or directory ~~were changed~~.

3. (Currently Amended): The method of claim 1, wherein said filtering ~~step outputs an~~ further comprises providing the event [[if]] to the determining a filename for each event comprising a ~~the parameters indicate~~ parameter indicating opening ~~that~~ a file ~~was opened~~ for truncation.

4. (Currently Amended): The method of claim 1, wherein said filtering ~~step outputs~~ further comprises providing the event to the determining a filename for each event comprising a parameter indicating modification ~~an event if the parameters indicate that~~ of the ownership or group ownership of a file ~~has been changed~~.

5. (Currently Amended): The method of claim 1, further comprising ~~a create step which outputs~~ outputting an alert message [[if a]] for each renamed file [[was renamed]] including [[a]] the filename of the file ~~that was renamed~~ and [[a]] the new filename of ~~name that~~ the renamed file ~~was renamed to~~.

6. (Currently Amended): The method of claim 1, comprising configuring a ~~templates~~ template based on a list of files and directories to be included or excluded based on whether the files and directories are considered unmodifiable.

7-12. (Cancelled)

13. (Previously Presented) A computer-readable medium storing instructions which, when executed by a processor, cause the processor to implement the method steps of claim 1.

14. (Currently Amended) A system for detecting critical file changes, comprising:

a processor; and

a memory storing instructions which, when executed by the processor, cause the processor to route events to ~~an appropriate~~ a template, wherein the event ~~includes~~ comprises one or more parameters and the template comprises a sequence of connected logic nodes comprising

at least one input node, at least one filter node, and at least one output node, filter the event, based on the template, as ~~either~~ a possible intrusion based on one of the one or more parameters and either dropping the event or outputting the event, and create an intrusion alert [[if]] for each [[an]] event [[is]] output from the filter.

15. (Currently Amended) The system of claim [[14]] 20, wherein the instructions causing the processor to filter the event ~~include~~ comprise instructions causing the processor to ~~output an event if~~ provide the event to the determine a filename instructions for each event comprising one of the one or more parameters ~~indicate that~~ indicating modification of the permission bits on a file or directory ~~were changed~~.

16. (Currently Amended) The system of claim [[14]] 20, wherein the instructions causing the processor to filter the event ~~include~~ comprise instructions causing the processor to ~~output an event if~~ provide the event to the determine a filename instructions for each event comprising one of the one or more parameters ~~indicate~~ indicating that a file was opened for truncation.

17. (Currently Amended) The system of claim [[14]] 20, wherein the instructions causing the processor to filter the event ~~include~~ comprise instructions causing the processor to ~~output an event if~~ provide the event to the determine a filename instructions for each event comprising one of the one or more parameters ~~indicate that~~ indicating modification of the ownership or group ownership of a file ~~has been changed~~.

18. (Currently Amended) The system of claim [[14]] 20, wherein the instructions further comprise instructions causing the processor to output an alert message ~~if a~~ for each renamed file, the alert message comprising ~~was renamed including a file that was~~ the filename of the file and the filename of the renamed file ~~and a new name that the file was renamed to~~.

19. (Currently Amended) The system of claim [[14]] 20, wherein the instructions comprise instructions causing the processor to configure a template ~~templates~~ based on a list of files and directories to be included or excluded based on whether the files and directories are considered unmodifiable.

20. (New) The system of claim 14, wherein the instructions causing the processor to filter the event comprise instructions causing the processor to determine a filename based on the event and output the event for each event indicating modification of a critical file based upon the determined filename.